al. and Cheung and further in view of Powar and Cochinwala et al. Claim 18 has been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Cheung and further in view of "The GSM Method" (Mouly et al.). Claims 21-23 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Cheung and further in view of Powar and Cochinwala et al.

The Examiner indicates that claims 5, 6 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

By the present response, Applicants have amended the specification to further clarify the invention. Moreover, Applicants have amended claims 1, 4, 9, 10, 13, 14 and 19 to further clarify the invention. Claims 1-23 remain pending in the present application.

Allowable Subject Matter

Applicants thank the Examiner for indicating that claims 5, 6 and 8 contain allowable subject matter.

Specification Objections

The disclosure has been objected to because of informalities. Applicants have amended the specification to further clarify the invention and respectfully request that this objection be withdrawn.

Claim Objections

Claim 10 has been objected to because of informalities. Applicants have amended claim 10 to further clarify the invention and respectfully request that this objection be withdrawn.

35 USC §112 Rejections

Claims 1, 3 [sic], 4 and 9 have been rejected under 35 USC §112, second paragraph. Applicants have amended the claims to further clarify the invention and respectfully request that these rejections be withdrawn.

35 USC §103 Rejections

Claims 1 and 12 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. in view of Diffie et al. Applicants respectfully traverse these rejections.

Pierce et al. discloses a communication system that employs a method of messaging between a subscriber unit and an infrastructure communications center. A messaging key associated with a subscriber unit reference number is provided to the subscriber unit and to the infrastructure communications center. An authentication key and/or an identifier for the subscriber unit is then produced by either the subscriber unit or the infrastructure communication center. The authentication key and/or the identifier is encrypted with the messaging key and is subsequently communicated, between the subscriber unit and the infrastructure communication center.

Diffie et al. discloses a method and apparatus for privacy and authentication in a mobile wireless network where a secure wireless communication link is provided between a mobile device and a base computing unit. Each participant node in the protocol generates a public key/private key pair. The private key is kept securely by the owner of the key. The public key is submitted over a secure channel to a trusted certification authority (CA). The CA examines the relevant information to ascertain that the public key is indeed being presented by someone whose identity is known and who can be "trusted". Having submitted the public key, the person submitting is assumed to be in a position to obtain credentials on behalf of the machine whose public key is being certified. The CA will then issue a certificate to the person (who is acting on behalf of the machine). The certificate will contain a binding between the public key and a logical identifier of the machine (such as a machine name), in the form of a document digitally signed using the CA's private key. In Diffie et al., the mobile device sends host certificate to the base computing unit along with a random challenge and a list of supported shared key algorithms. The base computing unit verifies the certificate that is digitally signed by the trusted CA. If the certificate is not valid, then the base computing unit rejects the connection attempt.

Regarding claim 1, Applicants submit that neither Pierce et al. nor Diffie et al., taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of this claim of, inter alia, a method for identifying a mobile station to a service provider that includes accessing a gateway by the mobile station and transmitting an identification code for mobile station to the gateway, verifying the identity of the mobile station by a gateway by accessing an authentication center and comparing mobile station generated variables computed by the mobile station and gateway generated variables computed by the gateway, delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station have been verified, or transmitting a digital signature by the mobile station accompanied by the digital certificate for a signature verification key to said service provider. Pierce et al. does not disclose or suggest anything related to identifying a mobile station to a service provider. The Examiner asserts that the limitations of verifying the identity of the mobile station by a gateway by accessing an authentication center and comparing mobile station generated variables computed by the mobile station and gateway generated variables computed by the gateway, in claim 1 of the present application are disclosed in Pierce et al. at col. 4, lines 25-35. However, this portion of Pierce et al. merely discloses that the infrastructure communication center receives an encrypted authentication key from a subscriber unit and stores the authentication key such that the authentication key corresponds with the previously stored subscriber unit reference number. This is not verifying the identity of a mobile station by a gateway by accessing an authentication center and comparing mobile station generated variable computed by the mobile station and gateway generated variables computed by the gateway, as recited in the claim of the present application. Neither Pierce et al. nor Diffie et al. disclose anything related to a mobile station generating variables and a gateway generating variables that are then compared for verification of a mobile station.

Regarding claim 12, Applicants submit that this claim is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons noted regarding independent claim 1.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of clams 1 and 12 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 2 and 7 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Diffie et al. and further in view of Cheung. Applicants respectfully traverse these rejections.

Cheung discloses system and method for increasing a value of an electronic payment card including performing a restore transaction in response to interruption of a value increase transaction.

Applicants submit that claims 2 and 7 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Cheung does not overcome the substantial defects noted previously regarding Pierce et al. and Diffie et al. Accordingly, Applicants submit that none of the cited references, taken alone, or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claims 2 and 7 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 9 and 10 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Diffie et al. and further in view of Powar. Applicants respectfully traverse these rejections.

Power discloses a secure interactive electronic accounts statement delivery system suitable for use over open networks such as the Internet. A certification hierarchy is utilized to ensure that electronic bills, invoices and other account statements can be securely sent over open networks. The participants in the system are a certification authority, certification banks, billers, and customers.

Applicants submit that claims 9 and 10 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Powar does not overcome the substantial defects noted previously regarding Pierce et al. and Diffie et al. Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 9 and 10 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 11 and 13 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al., Diffie et al., Powar and further in view of Cochinwala et al. Applicants respectfully traverse these rejections.

Cochinwala et al. discloses a method using a telephone calling card to transact commerce electronically. A user initiates a phone call to a merchant using a calling card provided by a service provider. The service provider initially checks the identity of the user through the use of a PIN code. Once the user's identity is validated the user's call to the merchant is established. The user and merchant then agree upon the sale of an item at which time an invoice is provided to the service provider by the merchant. The invoice is then approved by the user while the merchant is disconnected from the call.

Applicants submit that claims 11 and 13 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Cochinwala et al. does not overcome the substantial defects noted previously regarding Pierce et al. and Diffie et al. Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 11 and 13 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 14, 15, 19 and 20 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. in view of Cheung. Applicants respectfully traverse these rejections.

Regarding claims 14 and 19, Applicants submit that neither Pierce et al. nor Cheung, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, inter alia, a system or computer program for ordering, authorizing and delivering goods and services using a mobile station that includes a GSM authentication module to verify that the mobile station is permitted to access a telecom structure, a mobile station certificate acquisition module to request a digital certificate for the mobile station from a gateway, or a gateway certificate generation module to verify that the mobile station is authorized to receive the digital certificate by transmitting an international mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match. The Examiner asserts that Pierce et al. discloses a GSM authentication module to verify that the mobile station is permitted to access a telecom infrastructure at col. 4, lines 25-35. However, as noted previously, this portion of Pierce et al. merely discloses the receiving and storing of the encrypted authentication key from the subscriber unit by the infrastructure communication center. This portion of Pierce et al. does not disclose a GSM authentication module or code segment used for verification, but merely discloses a process for receiving and storing. The Examiner further asserts that Pierce et al. discloses a gateway certificate generation module, as recited in the claims of the present application, in Pierce et al. at col. 3, lines 53-56 and 61-64. However, these portions of Pierce et al. merely disclose that a messaging and associated subscriber unit reference number are provided to the subscriber unit and/or infrastructure communication center depending on where the messaging key was produced, and that if the subscriber unit generated the messaging key, the messaging key may be transmitted to the infrastructure communication center using a RF link. This is not a gateway certificate generation module or code segment that verifies that a mobile station is authorized to receive a digital certificate. The Examiner admits that Pierce et al. does not disclose a gateway certificate generation module or code segment that calculates and compares variables in the way recited in the claims of the present application, but asserts that Cheung discloses these limitations in the claims of the present application at col. 3, lines 47-51, 63-64 and col. 4, lines 1-11. However, these portions of Cheung merely disclose the control means 11 being arranged to send and receive messages using appropriate communication protocols, a challenge-signed response procedure as shown in Fig. 2, and the process of security module 12 authenticating card 2 where card 2 calculates a message authentication code based on a random number identification data and sends it to the security module 12 that performs the same calculation to verify that the card is authentic. These portions of Cheung do not disclose or suggest anything related to an authentication center, transmitting an international mobile subscriber identifier received from a mobile station to the authentication center by a gateway certificate generation module, or calculating variables based on information received from the authentication center and comparing them to variables computed by a mobile station and issuing a digital certificate to the mobile station when the variables match, as recited in the claims of the present application.

Regarding claims 15 and 20, Applicants submit that these claims are dependent on independent claims 14 and 19, respectively, and, therefore, are patentable at least for the same reasons noted regarding these independent claims.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 14, 15, 19 and 20 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 16 and 17 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al., Cheung, Powar and Cochinwala et al. Applicants submit that these claims are dependent on independent claim 14 and, therefore, are patentable at least for the same reasons note previously regarding this independent claim. Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest, or render obvious the limitations in the combination of each of claims 16 and 17 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claim 18 has been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Cheung and further in view of Mouly et al. Applicants respectfully traverse this rejection.

Mouly et al. discloses the security related functions of GSM. Applicants submit that claim 18 is dependent on independent claim 14 and, therefore, is patentable at least for the same reasons noted previously regarding this independent claim. Applicants submit that Mouly et al. does not overcome the substantial defects noted previously regarding Pierce et al. Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 18 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claims 21-23 have been rejected under 35 USC §103(a) as being unpatentable over Pierce et al. and Cheung and further in view of Powar and Cochinwala et al. Applicants submit that these claims are dependent on independent claim 19 and, therefore, are patentable at least for the same reasons noted previously regarding this independent claim. Accordingly, Applicants that none of the cited references, taken alone, or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 21-23 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants respectfully submit that claims 1-23 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned **"Version with markings to show changes made."**

To the extent necessary, Applicant petitions for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees and excess claim fees, to Deposit Account No. 01-2135 (referencing case No. 0173.38633X00) and please credit any excess fees to such deposit account.

Respectfully submitted,

Frederick D. Bailey
Registration No. 42,282
ANTONELLI, TERRY, STOUT & KRAUS, LLP

FDB/pay
(703) 312-6600

Version with markings to show changes made

IN THE SPECIFICATION

Please substitute the following for the paragraph starting on page 6, line 17.

--Further, an embodiment of the present invention creates a system and computer program for ordering, paying for and delivering goods and services using a mobile station. This system and computer program uses a Global System for Mobile Communications (GSM) authentication module to verify that the mobile station belongs to a user that can be billed. It also has a mobile station certificate acquisition module to request a digital certificate for the mobile station from a gateway and verify that the gateway is authorized to issue the digital certificate by comparing variables computed by the gateway and the mobile station. The system and method also has a gateway certificate generation module to verify that the mobile station is authorized. This module also transmits an international mobile subscriber identifier received from the mobile station to an authentication center, and receives information [using] which it can use to verify the authenticity of the mobile station by means of a challenge-response protocol. Once verified, this module generates and issues a digital certificate to the mobile station.--

IN THE CLAIMS

Please amend the claims as follows:

1. (Twice Amended) A method for identifying a mobile station to a service provider, comprising:

accessing a gateway by the mobile station and transmitting an identification code for mobile station to the gateway;

verifying the identity of the mobile station by the gateway by accessing an authentication center and comparing mobile station generated variables computed by the mobile station and gateway generated variables computed by the gateway;

delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station have been verified; and

transmitting a digital signature by the mobile station accompanied by the digital certificate for a signature verification key to said service provider.

4. (Twice Amended) The method recited in claim 3, where [the] an integrity key (IK) is transmitted by the authentication center to the gateway.

9. (Amended) The method recited in claim 1, wherein [requesting a product or service from a seller and] transmitting the digital signature, accompanied by the digital certificate for the signature verification key [as payment to the seller] to said service provider, further comprises:

transmitting the certificate with [the] a request for [the] a product or service;

receiving an invoice from [the] a seller indicating a price for the product or service;

computing a digital signature on the invoice;

approving the invoice by transmitting the digital signature to the seller; and

accepting delivery of the product or service by [the] a buyer.

10. (Amended) The method recited in claim 9, wherein the seller upon transmission of the digital signature, further comprises:

verifying the digital signature;

verifying that restrictions associated with the digital certificate are not violated; and

creating [the] an accounting record for the product or service sold.

13. (Amended) The method recited in claim 11, wherein delivering a digital certificate to the mobile station by the gateway when the identify of the mobile station and the gateway have been verified, further comprises:

requesting a digital certificate by the mobile station from the gateway sued to order and [pay for] authorize a product or service from a seller.

14. (Amended) A system for ordering, [paying for] authorizing and delivering goods and services using a mobile station, comprising:

a GSM authentication module to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition module to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation module to verify that the mobile station is authorized to receive the digital certificate by transmitting an international mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match.

19. (Amended) A computer program embodied on a computer readable medium and executable by a computer for ordering, [paying for] authorizing and delivering goods and services using a mobile station, comprising:

a GSM authentication code segment to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition code segment to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation code segment to verify that the mobile station is authorized to receive the digital certificate by transmitting an international mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match.